					Insira aqui a designação da entidade jurídica registada							
Número do documento: P16					Título do documento: **Política de Mascaramento e Pseudonimização de Dados**							
Versão: 1.0		Data de entrada em vigor: 01.01.2025			Proprietário do documento:							
X	Política		Norma		Procedimento		Formulário		Registo		Outro	

Histórico de revisões				
Número da revisão	**Data da revisão**	**Alterações**	**Revisto por**	**Proprietário do processo**

Aprovações			
Nome	**Cargo**	**Data**	**Assinatura**

Alinhamento com normas e regulamentos

Norma/Regulamento	Cláusula/Artigo	Comentário
ISO/IEC 27001:2022	Cláusula 6.1	Requisitos gerais de gestão de riscos e controlos operacionais aplicáveis ao mascaramento e à pseudonimização
ISO/IEC 27002:2022	Controlos 8.11, 8	Orientações de controlo sobre a implementação de mascaramento e pseudonimização
NIST SP 800-53 Rev.5	PM-17, PT-2, PT-3, SC-12, SC-28, SC-30	Controlos de privacidade e confidencialidade para minimização de dados, transformação e limitação de acesso
RGPD da UE	Artigos 4(5), 5(1)(c,f), 32	Base jurídica e requisitos para pseudonimização e medidas de proteção de dados
Diretiva NIS2 da UE	Artigo 21(2)(c)	Obrigação de adotar medidas técnicas e organizativas, incluindo tecnologias de reforço da privacidade (PETs)
DORA da UE	Artigos 10(1), 10(2)(e)	Gestão do risco das TIC e controlos de confidencialidade aplicáveis ao mascaramento e à pseudonimização de dados
COBIT 2019	DSS05.01, DSS06.06, MEA	Controlos de governação para a proteção de dados através de mascaramento e avaliação da conformidade

1. Finalidade

1.1 Esta política define a abordagem da organização à implementação de mascaramento e pseudonimização de dados enquanto tecnologias de reforço da privacidade (PETs), com o objetivo de reduzir a identificabilidade e a exposição de dados pessoais ou sensíveis.

1.2 Esta política suporta a utilização segura da informação em testes, analítica e operações, assegurando simultaneamente o cumprimento dos requisitos legais e regulamentares, a mitigação do impacto de violações e a aplicação dos princípios de minimização de dados e de confidencialidade.

1.3 A política está alinhada com a ISO/IEC 27001:2022, suporta o artigo 4(5) do RGPD da UE relativo à pseudonimização e integra uma implementação baseada no risco, consistente com as normas NIST, a Diretiva NIS2 da UE, o DORA da UE e o COBIT 2019.

2. Âmbito

2.1 Esta política aplica-se a:

2.1.1 Todos os trabalhadores, prestadores de serviços, terceiros ou fornecedores com acesso a sistemas que tratem informação pessoal, confidencial ou sensível.

2.1.2 Todos os ambientes de dados, incluindo produção, desenvolvimento, teste e pré-produção.

2.1.3 Todas as formas de mascaramento de dados (por exemplo, estático, dinâmico, determinístico, tokenização) e técnicas de pseudonimização utilizadas para reduzir riscos de privacidade.

2.1.4 Todos os tipos de dados (estruturados ou não estruturados), sistemas (locais ou alojados na nuvem) e aplicações que envolvam dados pessoais ou sujeitos a regulamentação.

2.2 O âmbito inclui a utilização em:

2.2.1 Desenvolvimento de aplicações e ambientes de QA/testes

2.2.2 Plataformas de analítica ou de reporte

2.2.3 Troca de dados com terceiros ou prestadores de serviços terceiros

2.2.4 Sistemas de cópia de segurança, arquivo ou recuperação

3. Objetivos

3.1 Assegurar a aplicação consistente e eficaz de mascaramento e pseudonimização para reduzir os riscos de exposição ou utilização indevida de dados.

3.2 Assegurar que dados reais nunca são utilizados em ambientes de não produção, salvo se tiverem sido transformados através de técnicas PET aprovadas.

3.3 Manter a integridade referencial, a usabilidade e as transformações com preservação do formato, quando exigido para consistência operacional.

3.4 Aplicar controlos de acesso rigorosos aos dados originais, aos dados mascarados e às chaves de reidentificação.

3.5 Tratar os conjuntos de dados mascarados ou pseudonimizados como dados sensíveis, sujeitos a registo de acessos, controlos de retenção e protocolos de resposta a incidentes.

3.6 Validar a eficácia destes controlos através de testes contínuos, monitorização e procedimentos de auditoria.

4. Papéis e responsabilidades

4.1 Alta Direção

4.1.1 Aprova esta política e assegura a sua aplicação no contexto mais alargado das iniciativas de governação de TI e de proteção de dados.

4.2 Diretor de Segurança da Informação (CISO) / Gestor do SGSI

4.2.1 Supervisiona a implementação e o cumprimento contínuo.

4.2.2 Assegura o alinhamento com a cláusula 6.1.3 da ISO/IEC 27001 (tratamento de riscos) e a cláusula 8.1 (controlo operacional).

4.2.3 Revê os registos de auditoria e valida a eficácia dos controlos.

[... As secções 4.3–8 não estão incluídas nesta pré-visualização. Adquira o documento completo para aceder ao conteúdo integral. ...]

9. Requisitos de revisão e atualização

9.1 Esta política deve ser revista, pelo menos, anualmente ou antes, em caso de:

9.1.1 Alterações regulamentares que afetem o mascaramento ou a pseudonimização

9.1.2 Adoção de novos sistemas de TI que tratem dados sensíveis

9.1.3 Alterações materiais ao esquema de classificação da organização

9.1.4 Constatações de auditoria que indiquem deficiências de controlo

9.1.5 Surgimento de novas ameaças ou tecnologias de mascaramento

9.2 O Gestor do SGSI deve liderar a revisão em consulta com o EPD, os Proprietários dos Dados, a Segurança de TI e a assessoria jurídica. As atualizações devem estar sujeitas a controlo de versões, ser aprovadas pela Direção Executiva e comunicadas a todas as partes interessadas afetadas.

10. Políticas relacionadas e articulações

10.1 P13 - Política de Classificação e Rotulagem de Dados. As decisões de mascaramento e pseudonimização dependem diretamente da classificação dos campos de dados e dos níveis de sensibilidade definidos na P13.

10.2 P14 - Política de Retenção e Eliminação de Dados. Os conjuntos de dados transformados devem ser retidos e eliminados de acordo com as regras do ciclo de vida definidas na P14, assegurando que os dados mascarados e pseudonimizados são tratados como sensíveis.

10.3 P17 - Política de Proteção de Dados e Privacidade. Estabelece os princípios de privacidade e as bases regulamentares para a aplicação da pseudonimização como atividade de tratamento conforme com o RGPD da UE e legislação semelhante.

10.4 P22 - Política de Registo e Monitorização. Permite a auditoria centralizada e a geração de alertas sobre eventos de mascaramento e pseudonimização, em conformidade com protocolos estruturados de monitorização de segurança.

11. Normas e quadros de referência

11.1 ISO/IEC 27001

11.1.1 Cláusula 6.1.3 - plano de tratamento de riscos: estabelece o mascaramento e a pseudonimização como mecanismos de tratamento de risco para reduzir a identificabilidade de dados sensíveis em ambientes de tratamento não essenciais.

11.1.2 Cláusula 8.1 - planeamento e controlo operacionais: determina controlos técnicos e processuais para a transformação segura de dados durante o tratamento, armazenamento ou transferência.

11.2 ISO/IEC 27002:2022

11.2.1 Controlos 8.11, 8: orientações sobre mascaramento e pseudonimização de dados para minimizar riscos de reidentificação e fuga de dados.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-17 - Proteção de informações pessoais identificáveis (PII): implementação de tecnologias de reforço da privacidade, como mascaramento e pseudonimização.

11.3.2 PT-2, PT-3: minimização e segurança do tratamento de informações pessoais identificáveis (PII) - transformação para reduzir a identificabilidade e aplicar controlo de acesso.

11.3.3 SC-12, SC-28, SC-30: confidencialidade e integridade dos dados - controlos de confidencialidade e ofuscação para armazenamento, transmissão e utilização.

11.4 RGPD da UE (2016/679)

11.4.1 Artigo 4(5): definição formal de pseudonimização.

11.4.2 Artigo 32: segurança do tratamento - medidas organizativas e técnicas para pseudonimização.

11.4.3 Artigo 5(1)(c,f): minimização de dados e confidencialidade através de pseudonimização/mascaramento.

11.5 Diretiva NIS2 da UE (2022/2555)

11.5.1 Artigo 21(2)(c): exige PETs como mascaramento e pseudonimização enquanto medidas de segurança.

11.6 DORA da UE (2022/2554)

11.6.1 Artigo 10(1): o quadro de gestão do risco das TIC inclui controlos de mascaramento/pseudonimização.

11.6.2 Artigo 10(2)(e): determina a utilização de tecnologias de transformação para proteger dados pessoais e financeiros.

11.7 COBIT 2019

11.7.1 DSS05.01: proteger ativos de informação - requisitos para mascaramento e pseudonimização.

11.7.2 DSS06.06: testes e analítica seguros - mascaramento em ambientes fora de produção.

11.7.3 MEA03: monitorização da conformidade quanto à eficácia do mascaramento e da pseudonimização.